UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,680,271 B2
APPLICATION NO. : 10/587460
DATED : March 16, 2010
INVENTOR(S) : Louis Guillou and Jean-Jaques Quisquater

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 11, Line 66, “in challenges d_l, d_2,...,d_m,” should read --m challenges d_1, d_2,...,d_m--

Column 12, Line 4, “to the controller, and” should read --to the processor-implemented controller, and--

Column 12, Line 15, “chooses at random in integers” should read --chooses at random m integers--

Column 12, Line 19, “producing a word of in bits” should read --producing a word of m bits--

Column 12, Line 63, “or the relationship G_i x Q_{iv} = 1 mod n” should read --or the relationship G_i x Q_{iv} = 1 mod n,--

Column 13, Line 18, “to any of claims 5-8 claim 6” should read --to claim 6--

Column 14, Line 17, “arranging, by processor,” should read --arranging, by the processor--

Column 14, Line 22, “arranging by processor, each public key G_i (where i = 1,...,m to” should read --arranging by the processor, each public key G_i (where i = 1 ,...,m) to--

Signed and Sealed this
Twenty-second Day of February, 2011

David J. Kappos

David J. Kappos
Director of the United States Patent and Trademark Office